

# Automated System to Anticipate Sand Piracy Using RFID and Load Sensor

A. Priya<sup>1</sup>, R. Ajith Singh<sup>2</sup>, E. Ezra David<sup>3</sup>, S. Aravind Durai<sup>4</sup>, P. Annavi<sup>5</sup>

<sup>1</sup>Assistant Professor, <sup>2,3,4&5</sup>UG Scholars

Electronics and Communication Engineering,  
K. Ramakrishnan College of Technology

**Abstract**—This paper describes about how to anticipate sand piracy in automated system. This system automatically opens and closes the gate when the vehicles enter/leave to the riverbed. The RFID tag and reader counts number of times the vehicle involved in mining process. The load sensor measures the load in the vehicle after filling the truck. If the weight exceeds the allowed weight and/or the vehicle enters more than the allowed number of times the gate will be closed. The database is maintained for the driver's fingerprint. The fingerprint of the driver is captured while leave from the riverbed and it is used to further process if the driver involved in sand smuggling.

**Keywords**—RFID tag and reader; load sensor; finger print scanner; e-gate; sand piracy

## I. INTRODUCTION

Illegal sand piracy is done on river beds and basins. It has been an serious problem since for the past twenty five years of 21<sup>st</sup> century and being continued till present. Although many laws and acts has been introduced to save sand from artificial erosion, Government could not stop the piracy due to corrupted officers. The main objective of this project is to prevent sand piracy using RFID tag and readers interconnected with load sensor and Fingerprint scanners where the system is in complete automation.

Sand mining is also known as heavy mineral mining, which can be explained as physical extraction of sand after which it is processed in pre concentration plants, to separate the mineral particles from the sand. But, most people confuse this activity with illegal sand mining.

This is because nobody pays attention to the activity which is conducted after the separation processes are over. After the separation is done, the sand particles which are of no use to the heavy mineral mining company is thrown back on the beach from where it was taken.

In fact, because of these misconceptions, even the government sometimes fails to understand this industry. Top companies in the heavy mineral mining industry are suffering a lot due to these misunderstandings because most people believe that these heavy mineral mining companies hoard sand.

Illegal beach mining includes mining of raw sand for the purpose of construction and other uses without taking

necessary permissions from the government authorities. It may also include mining of minerals from the sand for which the Government has not granted license.

## II. EXISTING TECHNOLOGIES

This work presents the concept and methodology as well as the architecture and physical implementation of an integrated node for smart-city applications. The presented integrated node lies on active RFID technology whereas the use case illustrated, with results from a small-scale verification of the presented node, refers to common-type waste-bins. The sensing units deployed for the use case are ultrasonic sensors that provide ranging information which is translated to fill-level estimations; however the use of a versatile active RFID tag within the node is able to afford multiple sensors for a variety of smart-city applications.

The most important benefits of the presented node are power minimization, utilization of low-cost components and accurate fill-level estimation with a tiny data-load fingerprint, regarding the specific use case on waste-bins, whereas the node has to be deployed on public means of transportation or similar standard route vehicles within an urban or suburban context.

## III. PROPOSED SYSTEM

This project is used to introduce a new system to prevent the smuggling of sand in automation. It counts the number of times the vehicle crossing the check post with the load and does not allow the vehicle to enter when it occurs more than the approved count. It does not allow the vehicle if it carries the excessive weight. The RFID is fixed in the vehicle. The weight of the vehicle is measured using load sensor. The number of loads of the vehicle is being counted using the RFID. It informs the concerned authority about the details of the vehicle in case if the vehicle carries excess load than the approved weight and count. Fingerprint sensor is used for security purpose and also to identify the person who drives the truck. In this project the power supply unit used for convert the Home appliances voltage into +5V/+12V according to the application. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.

#### IV. RELATED WORKS

In this first category, Load cell use is related to product, component, and/or system research, development and testing. The load sensors are commonly used for new hardware design testing and requirements verification, force distribution analysis, determination of operational forces, as well as overload or structural capabilities. In addition, many times the load cells are used to capture actual load and force data to fine tune or validate computer modeling and simulation tools, which are becoming more and more commonplace as a design tool for new hardware development.

The second category of usage, is not related to new or existing hardware design or testing, but is focused on product or process control applications. In these cases, the load cell products are used to control a certain force or operation to ensure a desired force is achieved either by direct monitoring or integrated into a complete feedback automated system.

Radio-Frequency Identification uses electromagnetic fields to automatically identify and track tags attached to objects. RFID tags are used in many industries, for example, an RFID tag attached to an automobile during production can be used to track its progress through the assembly line; RFID-tagged pharmaceuticals can be tracked through warehouses; and implanting RFID microchips in livestock and pets allows positive identification of animals.

Since RFID tags can be attached to cash, clothing, and possessions, or implanted in animals and people, the possibility of reading personally-linked information without consent has raised serious privacy concerns. These concerns resulted in standard specifications development addressing privacy and security issues.

ISO/IEC 18000 and ISO/IEC 29167 use on-chip cryptography methods for intractability, tag and reader authentication, and 20248 specifies a digital signature data structure for RFID and barcodes providing data, source and read method authenticity.

Pattern based algorithms compare the basic fingerprint patterns (arch, whorl, and loop) between a previously stored template and a candidate fingerprint. This requires that the images can be aligned in the same orientation. To do this, the algorithm finds a central point in the fingerprint image and centers on that. In a pattern-based algorithm, the template contains the type, size, and orientation of patterns within the aligned fingerprint image.

Furthermore, there are two more steps to improve the best quality for the input image: minutiae extraction and false minutiae removal. The minutiae extraction was carried out by applying ridge thinning algorithm which was to remove redundant pixels of ridges. As a result, the thinned ridges of the fingerprint image are marked with a unique ID so that further operation can be conducted. After the minutiae extraction step, the false minutiae removal was also

necessary. The lack of the amount of ink and the cross link among the ridges could cause false minutiae that led to inaccuracy in fingerprint recognition process. Second, in identification mode the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective

#### V. BLOCK DIAGRAM

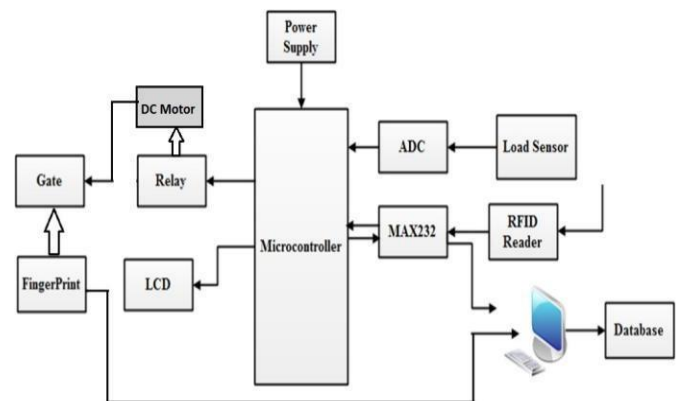


Fig.1. Block Diagram

The active RFID tag is fixed at the vehicle and when the vehicle enter into the sand mining location the RFID reader will reads the Tag and pass the information to the microcontroller. The RFID reader transmits the information in RS-232 format. It will not be supported by microcontroller so MAX232 is used to convert RS232 signal into TTL signal. The RFID reader will counts the number of times the vehicle entered to the gate. If the truck enters more than the authenticate/allowed times then the truck will be marked and the gate will be closed.

At the same time when the vehicle leaves from the mining location with the excessive amount of sand then the gate will be automatically closed. The load is measured by the load sensor and analog to digital converter converts the analog load value into the digital signal and its corresponding digital value is applied to the controller. The finger print of the driver is managing by the database to detect who drive the vehicle and to know who involves in a illegal activity. The person is identified by matching the finger print with Aadhar Unique Identification like database.

The schematic diagram for relay logic circuits are often called line diagrams, because the inputs and outputs are

essentially drawn in a series of lines. A relay logic circuit is an electrical network consisting of lines, or rungs, in which each line or rung must have continuity to enable the output device. A typical circuit consists of a number of rungs, with each rung controlling an output. This output is controlled by a combination of input or output conditions, such as input switches and control relays. The conditions that represent the inputs are connected in series, parallel, or series- parallel to obtain the logic required to drive the output. The relay logic circuit forms an electrical schematic diagram for the control of input and output devices. Relay logic diagrams represent the physical interconnection of devices.

A "database" refers to a set of related data and the way it is organized. Access to this data is usually provided by "database management system" (DBMS) consisting of an integrated set of computer software that allows users to interact with one or more databases and provides access to all of the data contained in the database (although restrictions may exist that limit access to particular data). The DBMS provides various functions that allow entry, storage and retrieval of large quantities of information and provides ways to manage how that information is organized.

A liquid crystal display (LCD) is a flat-panel display or other electronically modulated optical device that uses the light-modulating properties of liquid crystals. Liquid crystals do not emit light directly, instead using a backlight or reflector to produce images in color or monochrome. LCD's are available to display arbitrary images ( as in a general-purpose computer display) or fixed images with low information content, which can be displayed or hidden such as preset words, digits, and 7 – segment displays, as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements.

The conversion involves quantization of the input, so it necessarily introduces a small amount of error. Furthermore, instead of continuously performing the conversion, an ADC does the conversion periodically, sampling the input. The result is a sequence of digital values that have been converted from a continuous-time and continuous-amplitude analog signal to a discrete-time and discrete-amplitude digital signal. An ADC is defined by its bandwidth and its signal-to-noise ratio. The bandwidth of an ADC is characterized primarily by its sampling rate. The dynamic range of an ADC is influenced by many factors, including the resolution, linearity and accuracy (how well the quantization levels match the true analog signal), aliasing and jitter.

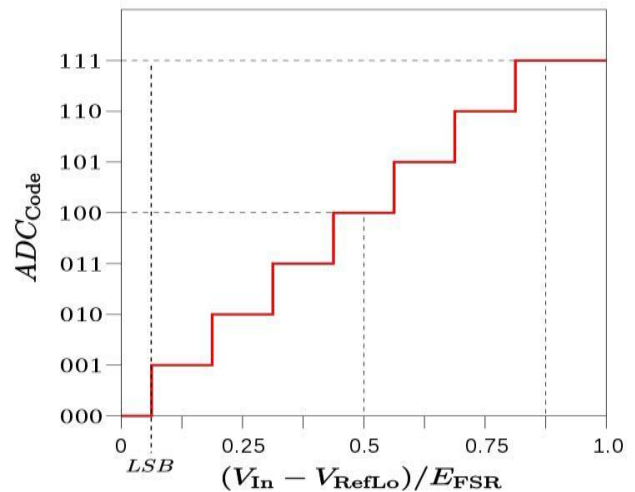
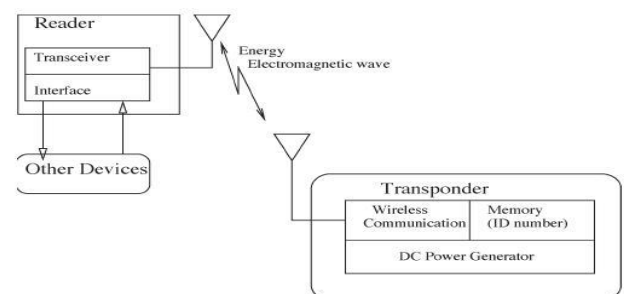


Figure 2: ADC conversion

## VI. COMPONENTS

### A. RFID SYSTEMS

RFID is an automatic identification technique which relies on data storage and transceiving of data using devices known as RFID tags or transponders. The power which is required to initiate the tag is transferred with the help of a contactless technology which is known as RFID reader. The mode of communication between the reader and the tag of an RFID system is based on radio frequency (RF) technology. A simplified RFID system is shown in Fig. 1. The tag includes the antenna within itself, which is responsible for providing communication while the reader is usually having one or two antennas. The reader which contains a transceiver generates a pulse of electromagnetic waves. The transponder receives the transmission which is further, rectified to get the dc power supply for the IC memory.



The processed signal transmitted by the transponder is then received by the reader again to obtain the tag's ID number. As the RFID technology is simple, more flexible and relatively cheaper it is nowadays gaining attention in a large number of applications, such as personal identification, food production control, security guard monitoring, and inventory management etc.

**a) RFID Reader**

UHF RFID readers basically are transceivers which perform the function of transmission and reception simultaneously that too at the same frequency. In order to increase the range of reading, readers are made to transmit in such a way that make use of maximum EIRP (Equivalent isotropically radiated power) using high gain directional antennas. But there has to be a proper isolation between transmit and receive channels in order to have reasonable good detection and decoding of weak tag signals.

Reader antenna is one of the important components of RF-ID system. The choice of antenna depends on maximum allowable radiated power and antenna beam width in UHF RF-ID bands. Now-a-days, RFID systems are using a wide variety of antennas such as switched beam antennas, polarization and space diversity antennas, smart antenna arrays etc. There are basically two types of antenna designs that are:

**Bistatic Antenna Configuration:**

The main feature of bistatic configuration is that it uses separate antenna for transmission and reception. This is shown in fig 2. These systems also make use of circularly polarized antennas. These systems find application in RFID portals and dock doors.

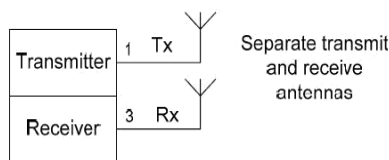


Figure 3: Bistatic Antenna

**Monostatic Antenna Configuration:**

In this type of configuration, there is only one antenna used for both transmission and reception purpose as shown in fig 3. They are not as good as bistatic configuration because they have poor isolation between transmit and receive channel.

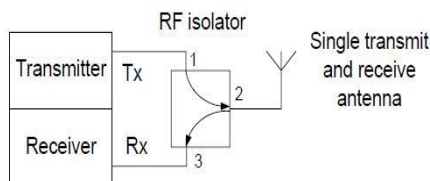


Figure 4: Monostatic Antenna

**b) RFID TAGS**

Two types of RFID tags are generally used. They are known as active and passive tags. Active RFID tags have a power source which helps them to have communication over a long

range, changeable data fields. The main problem of active RFID tags is that they are expensive and their duration of life is also less.

Active RFID tags help in manual sorting associated with switch lists. Active RFID tags have grown in applications where tagging and tracking is required. The main industries that are making use of active RFID tags are automotive, transportation, logistics, healthcare and military etc. Passive RFID tags on the other hand, stores the energy provided by the signal in a capacitor. This capacitor when properly charged is used as a power source for passive RFID tags. Passive RFID tags are having a short communication range but they are smaller and cheaper in size as compared to active RFID tags.

**B) LOAD SENSOR**

A load cell is a transducer that is used to create an electrical signal whose magnitude is directly proportional to the force being measured. The various types of load cells include hydraulic load cells, pneumatic load cells and strain gauge load cells.

Piezoelectric load cells work on the same principle of deformation as the strain gauge load cells, but a voltage output is generated by the basic piezoelectric material – proportional to the deformation of load cell. Useful for dynamic/frequent measurements of force. Most applications for piezo - based load cells are in the dynamic loading conditions, where strain gauge load cells can fail with high dynamic loading cycles.

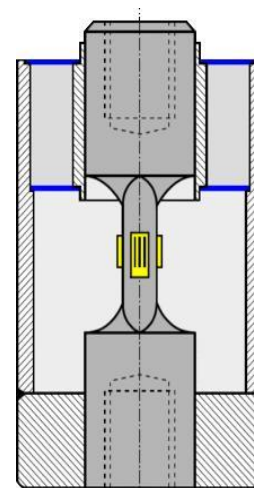


Figure 5: Load cell

It must be remembered that the piezoelectric effect is dynamic, that is, the electrical output of a gauge is an impulse function and is not static. The voltage output is only useful when the strain is changing and does not measure static values. However, depending on conditioning system used, "quasi static" operation can be done. Using a so-called "Charge amplifier " with "Long" time constant allow accurate measurement lasting many hours for large loads to many



minutes for small loads. Another advantage of piezoelectric load cell, conditioned with a Charge amplifier, is the wide measuring range that can be achieved. Users can choose a load cell with a range of hundred of kN and use it for measuring few N of forces with the same Signal/Noise ratio, again this is possible only with the use of a "Charge amplifier" conditioning.

### C) FINGERPRINT SCANNER

Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching.

Fingerprint processing has three primary functions: enrollment, searching and verification. Among these functions, enrollment which captures fingerprint image from the sensor plays an important role. A reason is that the way people put their fingerprints on a mirror to scan can affect to the result in the searching and verifying process. Regarding to verification function, there are several techniques to match fingerprints such as correlation-based matching, minutiae-based matching, ridge feature-based matching and minutiae-based algorithm. However, the most popular algorithm was minutiae based matching algorithm due to its efficiency and accuracy.

#### Minutiae based matching algorithm

The major minutia features of fingerprint ridges are ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.



Figure 6: Finger print

Pre-processing helped enhancing the quality of an image by filtering and removing unnecessary noises. The minutiae based algorithm only worked effectively in 8-bit gray scale fingerprint image. A reason was that an 8-bit gray fingerprint image was a fundamental base to convert the image to 1-bit image with value 0 for ridges and value 1 for furrows. As a result, the ridges were highlighted with black color while the furrows were highlighted with white color. This process partly removed some noises in an image and helped enhance the edge detection. Furthermore, there are two more steps to improve the best quality for the input image: minutiae

extraction and false minutiae removal. The minutiae extraction was carried out by applying ridge thinning algorithm which was to remove redundant pixels of ridges. As a result, the thinned ridges of the fingerprint image are marked with a unique ID so that further operation can be conducted. After the minutiae extraction step, the false minutiae removal was also necessary. The lack of the amount of ink and the cross link among the ridges could cause false minutiae that led to inaccuracy in fingerprint recognition process.

### d) MICROCONTROLLER

A microcontroller (or MCU for microcontroller unit) is a small computer on a single integrated circuit. In modern terminology, it is a System on a chip or SOC. A microcontroller contains one or more CPUs (processor cores) along with memory and programmable input/output peripherals. Program memory in the form of Ferroelectric RAM, NOR flash or OTP ROM is also often included on chip, as well as a small amount of RAM. Microcontrollers are designed for embedded applications, in contrast to the microprocessors used in personal computers or other general purpose applications consisting of various discrete chips.

Microcontrollers are used in automatically controlled products and devices, such as automobile engine control systems, implantable medical devices, remote controls, office machines, appliances, power tools, toys and other embedded systems.

By reducing the size and cost compared to a design that uses a separate microprocessor, memory, and input/output devices, microcontrollers make it economical to digitally control even more devices and processes. Mixed signal microcontrollers are common, integrating analog components needed to control non-digital electronic systems.

Some microcontrollers may use four-bit words and operate at frequencies as low as 4 kHz, for low power consumption (single-digit milliwatts or microwatts). They will generally have the ability to retain functionality while waiting for an event such as a button press or other interrupt; power consumption while sleeping (CPU clock and most peripherals off) may be just nanowatts, making many of them well suited for long lasting battery applications.

Other microcontrollers may serve performance-critical roles, where they may need to act more like a digital signal processor (DSP), with higher clock speeds and power consumption.

The MAX232 has two receivers that convert from RS-232 to TTL voltage levels, and two drivers that convert from TTL logic to RS-232 voltage levels. As a result, only two out of all RS-232 signals can be converted in each direction. Typically, the first driver/receiver pair of the MAX232 is used for TX and RX signals, and the second one for CTS and RTS signals. There are not enough drivers/receivers in the MAX232 to also connect the DTR, DSR, and DCD signals. Usually, these

signals can be omitted when, for example, communicating with a PC's serial interface.

### e) DC MOTOR

A DC motor is any of a class of rotary electrical machines that converts direct current electrical power into mechanical power. The most common types rely on the forces produced by magnetic fields. Nearly all types of DC motors have some internal mechanism, either electromechanical or electronic, to periodically change the direction of current flow in part of the motor.

DC motors were the first type widely used, since they could be powered from existing direct-current lighting power distribution systems. A DC motor's speed can be controlled over a wide range, using either a variable supply voltage or by changing the strength of current in its field windings.

The brushed DC electric motor generates torque directly from DC power Supplied to the motor by using internal commutation, stationary magnets (permanent or electromagnets), and rotating electrical magnets. Advantages of a brushed DC motor include low initial cost, high reliability, and simple control of motor speed. Disadvantages are high maintenance and low life-span for high intensity uses.

Typical brushless DC motors use one or more permanent magnets in the rotor and electromagnets on the motor housing for the stator. A motor controller converts DC to AC. This design is mechanically simpler than that of brushed motors because it eliminates the complication of transferring power from outside the motor to the spinning rotor.

## VII. FUTURE WORK

Our idea is to design a model of Automated System to Anticipate Sand Piracy Using RFID and Load Sensor. But in future we can implement as a real world system and we can also synchronize with large database so, the vehicle model, number plate and driver's finger print is verified by the data in the cloud storage for providing high security.

## VIII. CONCLUSION

In this paper we have expressed our idea to prevent the sand piracy and we have concluded that Government could not stop the piracy due to corrupted officers. So, we have designed an automated method to prevent the sand piracy and it will help to prevent our countries ores and minerals.

## REFERENCES

- [1] Glover, B., Bhatt, H., 2006. An Introduction to RFID, Chap. 1. RFID Essentials. 1. O'Reilly. 276
- [2] Flora Dilys Salim, Seng Wai Loke, Bala Srinivasan, Shonali Krishnaswamy "Collision Pattern Modeling and Real-Time Collision Detection at Road Intersections" Proceedings of the 2007 IEEE Intelligent Transportation Systems Conference Seattle, WA, USA, Sept. 30 - Oct. 3, 2007
- [3] Bichlien Hoang, Ashley Caudill "RFID" Originally published on the IEEE Emerging Technology portal 2006 - 2012. z
- [4] Gurjot Singh Gaba, Nancy Gupta, Gaurav Sharma, Harsimranjit Singh Gill "Intelligent Cars using RFID Technology" International Journal of Scientific & Engineering Research Volume 3, Issue 7, June-2012
- [5] Ateeth Kumar Thirukkovulur, Harikrishna Nandagopal, Vigneesh Parivallal "RFID Technology for Smart Vehicle Control using Traffic Signal & Speed Limit Tag Communication" International Journal of Computer Applications (0975 - 8887) Volume 43- No.14, April 2012
- [6] Samadi "Applications and Opportunities for Radio Frequency Identification (RFID) Technology in Intelligent Transportation Systems: A Case Study" International Journal of Information and Electronics Engineering, Vol. 3, No. 3, May 2013
- [7] "ZT-50-mini Active RFID Tag and ZR-USB Active RFID Reader." [Online]. Available: www.tagsense.com.
- [8] J. Luk'a's, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," Information Forensics and Security, IEEE Transactions on, vol. 1, no. 2, pp. 205-214, June 2006.
- [9] Mo Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor noise," Information Forensics and Security, IEEE Transactions on, vol. 3, no. 1, pp. 74-90, March 2008.
- [10] Y. Hu, B. Yu, and C. Jian, "Source camera identification using large components of sensor pattern noise," in Computer Science and its Applications, 2009. CSA '09. 2<sup>nd</sup> International Conference on, Dec 2009, pp 1-5.
- [11] A. Hinrichs and J. Vyb'ral, "Johnson-Lindenstrauss Lemma for Circulant Matrices," Random Struct Algorithms, vol. 39, no. 3, pp. 391-398, Oct. 2011.
- [12] F. Krahermer and R. Ward, "New and Improved Johnson-Lindenstrauss Embeddings via the Restricted Isometry Property," SIAM Journal on Mathematical Analysis, vol. 43, no. 3, pp. 1269-1281, 2011.
- [13] D. Valsesia and E. Magli, "Compressive signal processing with circulant sensing matrices," in Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on, May 2014, pp. 1015-1019.
- [14] Y.-L. Park, C. Majidi, R. Kramer, P. Bérard, and R. J. Wood, "Hyperelastic pressure sensing with a liquid-embedded elastomer," J. Micromech. Microeng., vol. 20, no. 12, p. 125029, Nov. 2010.
- [15] R. D. P. Wong, J. D. Posner, and V. J. Santos, "Flexible microfluidic normal force sensor skin for tactile feedback," Sensor. Actuat. APhys., vol. 179, pp. 62-69, Jun. 2012.
- [16] S. G. Yoon, H.-J. Koo, and S. T. Chang, "Highly stretchable and transparent microfluidic strain sensors for monitoring human body motions," ACS Appl. Mater. Interfaces, Vol. 7, no. 49, pp. 27562-27570, Nov. 2015.
- [17] W. Gu, J. Shen, Y. Yang, and Z. Hao, "Dynamic characterization of a polymer-based microfluidic device for distributed-load detection," Sensor. Actuat. A-Phys., vol. 222, pp. 102-113, Feb. 2015.
- [18] B. Nie, R. Li, J. D. Brandt, and T. Pan, "Microfluidic tactile sensors for three-dimensional contact force measurements," Lab Chip, vol. 14, no. 22, pp. 4344-4353, Nov. 2014.
- [19] Y. Ma, L.-H. Yeh, C.-Y. Lin, L. Mei, and S. Qian, "pH-Regulated ionic conductance in a nanochannel with overlapped electric double layers," Anal. Chem., vol. 87, no. 8, pp. 4508-4514, Mar. 2015.
- [20] R. Pratap, S. S. Mohite, and A. K. Pandey, "Squeeze film effects in MEMS devices," J. Indian Inst. Sci., vol. 87, no. 1, pp. 75-94, Jan.-Mar. 2007.
- [21] R. C. W. Leung, T. Thurber, and W. Ye, "On the modified Reynolds equation model for the prediction of squeeze-film gas damping in a low vacuum," Microfluid. Nanofluid., vol. 11, no. 6, pp. 753-762, Jul. 2011.
- [22] M.-J. Huang, L. Mei, L.-H. Yeh, and S. Qian, "pH-Regulated nanopore conductance with overlapped electric double layers," Electrochem. Commun., vol. 55, pp. 60-63, Jun. 2015.